Lessons from the Defence industry

Responsible cyber behaviour

RUSI

GLOBAL PARTNERSHIP FOR RESPONSIBLE CYBER BEHAVIOUR

Digital Intelligence

BAE SYSTEMS

Contents

Executive Summary

The necessity to understand and promote responsible behaviours within the Defence and Cyber sectors (i.e. the production and selling of cyber and defence capabilities for state use) has never been greater. The challenging global landscape coupled with the increasing velocity of modern warfare capabilities has highlighted a strong demand for responsibility in the production and distribution of both cyber and military services. Despite the Cyber Security sector emerging as one of the fastest growing industries[1] with broad capabilities that could risk national and shared interests[2], discussion of what it means to be a responsible industry player when developing cyber security services and products is still relatively underdeveloped.

The Defence sector, including companies including BAE Systems, have integrated cyber security as a core part of the commercial offering. Additionally, Defence contractors are well-positioned to consider questions of responsible cyber behaviour, because they have historically had to deal with and reflect on many questions concerning responsible and irresponsible use of military, and more recently, cyber capabilities. These provide us with strong parallels in the potential for misuse, proliferation and harm to individuals, society and governments. While the possible harms of cyber are not as clear cut as military capabilities, the interconnectedness of the global landscape and reliance on digital products in everyday use presents a different opportunity, but just as vital for Defence primes, to develop and continue practises from the Defence industry into Cyber markets.

> Drawing on BAE Systems' experience as the UK's largest Defence prime, this paper assesses how the Defence sector – one of largely established norms, regulations and governance – can provide lessons for the development of responsible cyber discourse and practice. Through interviews from industry, policymakers and academia, this paper identifies several mechanisms that serve as exemplars for what the Cyber sector could adopt from Defence.

This paper also examines the use of legal and non-legal mechanisms in the Defence industry compared to the Cyber sector. Legal tools, including legislation and export control regimes, demonstrate the government's role in ensuring strong regulation and enforcement of compliance through accountable measures: the backbone of responsible behaviour. Non-legal tools, including ethics and business standards, are also essential to ensure that the private sector can create common practices of good governance – along with increased transparency to eliminate ambiguity and reduce the risk of irresponsibility. Current discussions, including the Pall Mall Process, highlight an ambiguity around corporate responsibility that emphasises the need for collaboration across industry, government and academia.

Definitions of responsible behaviour are likely to evolve and mature to reflect the times. Legal and non-legal mechanisms can promote robust concepts of responsible behaviour into cyber discussions and, in turn, codify into coherent and broadly applicable business practices.

1 Introduction

1.1 About the Responsible Cyber Behaviour project and publication

Malicious activities by state and non-state actors in cyberspace present a continuous threat to international peace, stability and security. Geopolitical tensions often tend to favour a polarised view of what responsibility means in cyber and tech security, thus leaving out the important nuance as to how different regions and stakeholders perceive it.

In 2022, the Royal United Services Institute (RUSI) launched the Global Partnership for Responsible Cyber Behaviour (GP-RCB) – a platform for research and dialogue comprised of over 80 scholars from countries in Latin America and the Caribbean, North America, the Middle East and Africa, and the Indo-Pacific. The GP-RCB is a global research hub designed to enable evidence-based action on cyber policy and cyber security issues within international multilateral organisations.

To better inform practical steps that unblock the international debate on the application of rules, norms and principles in cyberspace, the GP-RCB focuses on understanding and identifying the varying approaches to cyberspace and technology taken by states in an increasingly fractured geopolitical landscape. The network responds to a notable fragmentation and knowledge gap in the global research community on Responsible Cyber Behaviour (RCB), marked by an inconsistent understanding of mechanisms, concepts and interpretations of responsibility, alongside a lack of clarity on what RCB means in practice.

1.2 Research Aim

The malicious use of information and communications technologies is far more complex than it was twenty years ago when the first set of cyber norms on responsible state behaviour were agreed by states at the UN.[3] Non-state actors – especially private companies – have become a core part of cyber security services and infrastructure provision. Therefore, from both a multilateral and threat-based perspective, this is an appropriate time to consider how the debate about responsible behaviour in cyberspace not only extends beyond the remit of national governments and multi-lateral organisations but most importantly, how different parts of the industry understand responsible cyber behaviour.

This research paper investigates the potential role of Defence companies in shaping responsible behaviours as a complement to the behaviours of nation states. To support fresh policy thinking on RCB, specifically drawing on BAE Systems' experience as a Defence prime, it seeks to identify parallels and lessons from the Defence sector that could inform both private sector and governmental approaches to responsible behaviours in the adjacent Cyber sector.

1.3 Approach

The Defence sector offers a number of parallels to the Cyber sector – a term used in this paper to encompass the UK Cyber sector and includes businesses that provide products or services that enable the protection of internet connected systems and their users[4], as well as cyber capabilities that might be used by states in cyber operations that advance strategic interests. Defence and Cyber share several similarities, such as the use of advanced technology, common suppliers, customer markets, export regulation, and a need to control the use of goods and services due to the potential for misuse. Defence also offers Cyber the chance to learn from the far greater domestic and international history of reflection and codification of responsible behaviour across the Defence sector.

This paper draws on several data collection methods including academic literature review, desk-based research, and interviews with those working in the Defence and Cyber sectors, academia, and government. Those contributing did so on condition of anonymity and so remarks have not been attributed to any individual organisations. The views expressed, therefore, should not be seen as representing the position of any single entity or that of the Defence or Cyber sectors.

This paper's focus is limited to exploring the primary factors that drive responsible behaviour in the Defence industry – chiefly domestic and international legislation, regulation, and commonly agreed principles (such as military ethics) – when it comes to the development and sale of capabilities. To make the most meaningful comparison between Defence and Cyber, this paper does not explore the impact of military culture and its model of leadership or exercising as part of the definitions of responsibility.

In addition, the paper is not focused on how Defence firms promote cyber security governance and practices throughout the development of their military platforms and tools (i.e. product security). The paper focuses on the production and distribution of cyber and defence capabilities and seeks to provide insights into the Cyber-Defence industrial nexus that can inform future research and policy reflections on the topic.

> Defence and Cyber share several similarities, such as the use of advanced technology, common suppliers, customer markets, export regulation, and a need to control the use of goods and services due to the potential for misuse.

2 Background

2.1 Why now?

This paper has been produced at an inflection point of Cyber's evolution and its place in the current political domain. As the UN Open Ended Working Group on Cyber (OEWG)[5] ends this year, and initiatives like the Pall Mall Process continue discussions on the proliferation and irresponsible use of cyber capabilities[6], it is timely to understand what Responsible Cyber Behaviour means for a range of actors.

The Cyber sector – including offensive and defensive capabilities – sits at a complex interplay of heightened geopolitical tensions and an increasingly challenging landscape. Cybercrime is projected to cost $13.82 trillion globally by 2028[7] and the proliferation of offensive cyber capabilities has increased the pressure on states to continue to invest and develop. Cyber capacities and capabilities provide an easy route for malicious actors to cause harm by exploiting vulnerabilities across organisations, supply chains, sectors and national borders.

> The emergence of new threats has increased the necessity for a more competitive market and expenditure across military and cyber – including investments and stronger governance.

The UK's Defence budget rose to £59.8 billion in 2025/26, with plans to increase to 2.5% of GDP by April 2027[8]. The UK also continues to build its vision as a global cyber power[9]. The National Cyber Security Centre is playing a leading role in cyber security at home and overseas while the National Cyber Force provides cyber operations in support of national security interests, collaborating with allies to ensure strategic cooperation[10] as well as designing principles for responsible cyber operations[11].

In parallel, under the Digital Europe Programme for the period 2021-2027, the EU committed €1.6 billion to cyber security capabilities[12] and established the European Cybersecurity Industrial, Technology and Research Competence Centre[13]. This highlights a growing effort and investment to ensure that cyberspace can be secured, with regulation where appropriate, to manage the diversity of cyber capabilities not previously recognised. Now more than ever, it is useful to reflect on non-state actors, such as the Defence industry, to understand what responsibility means to the private sector, how it should be employed, and the intersection between military and cyber services.

2.2 The Defence and Cyber marketplaces

The UK has one of the world's leading Defence industries with orders worth £14.5bn in 2023[14], dominated by aerospace products and services. The UK's Defence industry is shaped by government priorities and military requirements. It includes large private sector contractors and manufacturers building equipment, hardware, advanced electronics, communications, surveillance and cyber security solutions – all underpinned by a global supply chain. Looking more broadly, the US is dominated by a handful of major Defence primes while, as an economic zone, Europe comprises a more diverse – albeit fragmentated – market with around 15 major Defence primes[15] and thousands of small and medium sized enterprises. Barriers to entry into the Defence sector can be high, requiring significant capital investment, complex and lengthy development and procurement processes, strict national and international regulatory frameworks (primarily relating to export and compliance), and international collaboration. Firms tend to be large and well established; some have thousands of government security-cleared staff. With long-term contracts and dependence on government procurement cycles, growth tends to be stable; until 2022, UK exports were primarily destined for the Middle East[16]. Now they are concentrated on Europe and likely to grow further in this region[17], which will shape the demand and production of future military platforms.

Many large companies straddle both sectors, providing defence and cyber products and services. In the UK, for example, this includes BAE Systems, Rolls Royce, Leonardo, QinetiQ, Thales UK, Atos UK, and Babcock International. The broader Cyber sector is more diverse, with a myriad of small and medium sized businesses. The sector has grown rapidly since the 1990s, with rising demand for digital services. Initially focused largely on cyber security (such as antivirus software and firewalls), the market has expanded significantly over the last 15 years in line with the mushrooming use of the internet, social media, cloud services, and the dynamic threat landscape to include intrusive and offensive cyber capabilities[18]. That said, cyber security still dominates the UK market, representing roughly 65% of total UK security export revenue in 2023[19]. Due to the similarities in relation to national security between cyber operations and defence products including developing capabilities in offensive cyber, this paper will focus on this subsection of the Cyber sector in order to establish a comparison of how responsible behaviour has and will continue to develop in this space.

Though highly competitive and dependant on access to scarce expert resources, entering the Cyber market is simpler than becoming a Defence company. Upfront costs are lower, technology development is faster, and as the market is wider than government there are fewer barriers to entry (at least when compared with the Defence sector, where legal prerequisites are required to obtain government contracts, such as the Defence and Security Public Contracts Regulations 2011 (DSPCR)[20]. UK security exports have risen rapidly from £4.3bn in 2016 to £11bn in 2023[21]. Similar to defence exports, the majority of UK cyber exports by destination region were for Europe and North America.

2.3 Defining responsible behaviour

Responsible Cyber Behaviour (RCB), as defined in RUSI's RCB guide[22], refers to the collective expectations of state and non-state actors regarding how they should behave in cyberspace. Behaviour comprises the values, norms, policies, practices, and technologies that are intended to protect and secure cyberspace. These expectations are highly contested and differ across the globe. RUSI's RCB guide allowed a basis for comparing the Cyber sector with the Defence sector and the associated domain of armed conflict.

Core principles relating to armed conflict have long been embedded in international humanitarian and human rights laws, treaties and conventions, given effect via national legislation and regulation to control the development, sale, export and use of military and dual-use goods. Underpinning these core principles is the importance of necessity, proportionality and need to minimise harm to civilians and civilian property.

Interviewees engaged in our research highlighted that export control was one of the biggest drivers of responsible behaviour. Export control regimes and compliance offer a useful litmus test for what is deemed responsible practise in the development and distribution of capabilities, and what is deemed irresponsible and the appropriate penalties involved.

Whilst export control is a key factor in defining responsible behaviour, this paper recognises that other factors are also relevant, and proposes that responsible behaviour in the Defence industry should be understood through the following mechanisms:

1

Regulation

Rules that are robust and broad enough to outline what the Defence sector must do to be compliant, with distinctions for what is deemed irresponsible in relation to the national interests and international obligations capabilities are subject to.

2

Enforcement

Clear and proportionate enforcement of regulation, in which national governments set out penalties for non-compliance including the publication of fines and charges for violations of regulation that can include 'consent agreements' covering remedial measures.

3

Transparency

Defence contractors must operate with transparency when conducting their business, including in their operational frameworks and protection of sensitive information. This goes beyond simply compliance with regulation and includes ensuring accountability of all parties involved, such as the supplier, the customer and any third party.

4

Governance

Ensuring that firms have robust internal frameworks to govern responsible behaviours – necessary to ensure both regulatory compliance and responsibility more widely, e.g. relating to ethical standards of conduct.

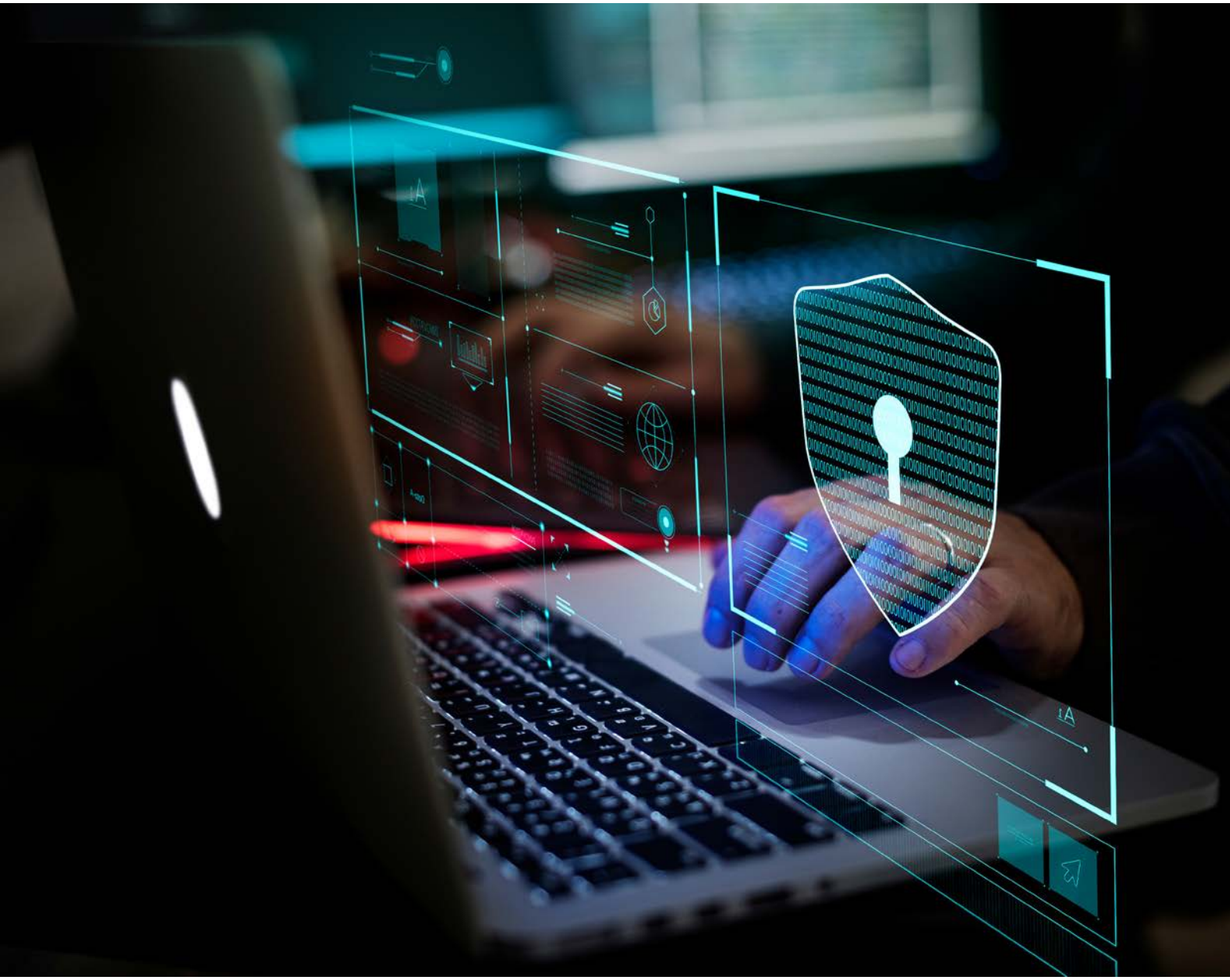
5

Collaboration

To stay relevant in an environment of technological advances and geopolitical changes, high level multi-stakeholder collaboration (including government, industry and academia) is essential to grow the discourse on how customers, trade bodies, policymakers and contractors remain responsible in the product lifecycle.

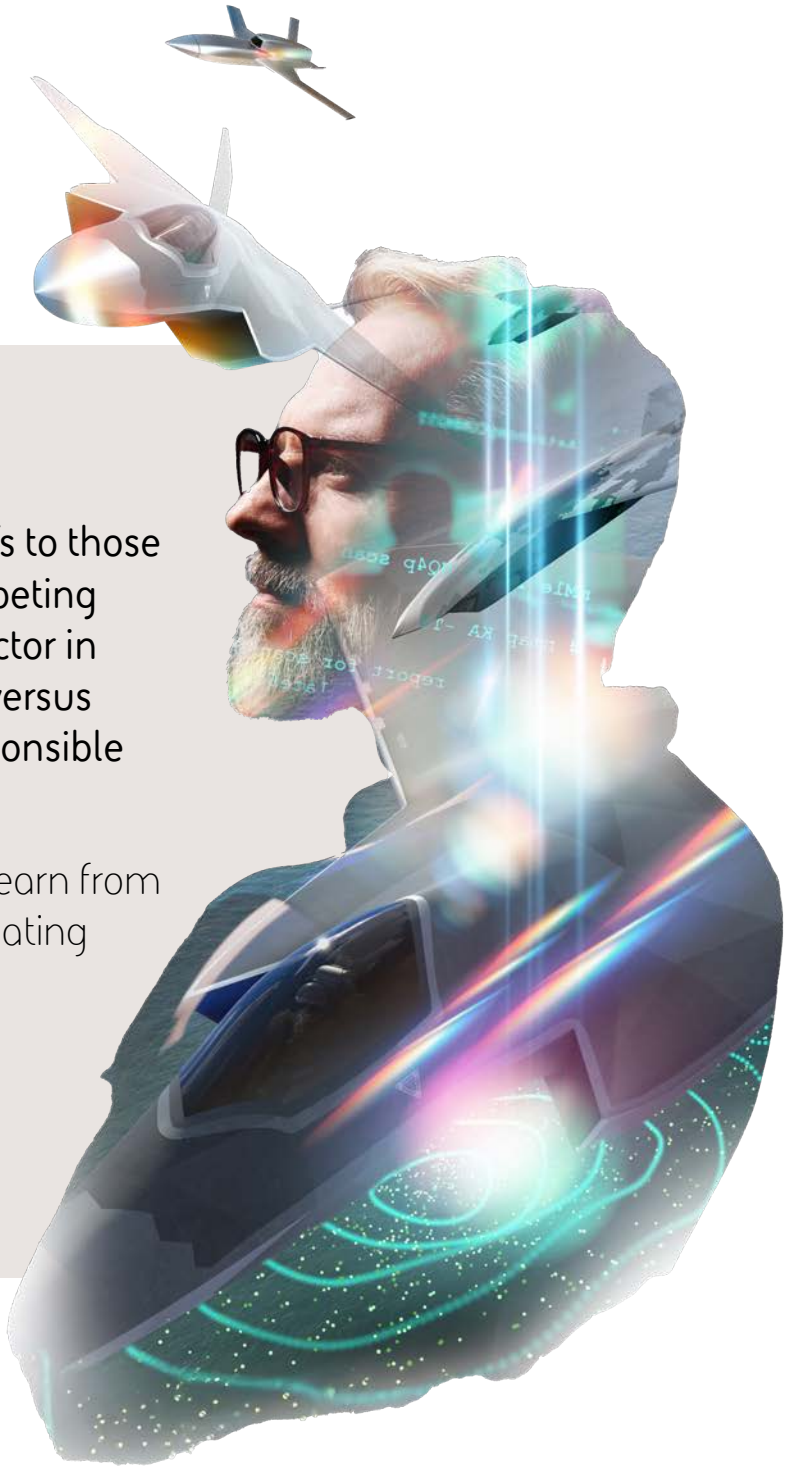
Though recognised as an important issue at the turn of the millennium[23], international efforts to define cyber operations and establish common views on responsible behaviour only slowly gained traction after 2010. It took a series of cyber incidents against Estonia in 2007[24], the Republic of Georgia in 2008[25] and Iran[26] (discovered in 2010) to demonstrate the destructive potential of cyber operations. It was at this point that the international community started to take the risk of cyber breaches and their consequent impact seriously.

Since then, discussion of Responsible Cyber Behaviour has grown in line with the development of cyber capabilities. Huge steps have been taken to codify thinking on this topic – notably via the UN framework of responsible state behaviour in cyber space, agreed in 2015[27], and via a swathe of international and national legislation that gave effect to norms designed to protect human rights in cyber space by placing increased protections on the privacy of personal information, such as the EU's GDPR in 2016[28]. A year after the devastating WannaCry ransomware attacks, the 2018 'Paris Call for Trust and Security in Cyberspace' represented the first major multi-stakeholder initiative that sought to involve private companies and civil society organisations in producing principles of expected cyber behaviour[29]. Focused primarily on establishing a defensive posture (e.g. protecting intellectual property, supply chains, electoral systems, the domain name system, infrastructure and individuals) these initiatives also included calls to promote international norms and the non-proliferation of intrusive cyber capabilities – developed further by the 2024 Pall Mall Process[30].



2.4 Responsible behaviour in the Defence sector

Challenges associated with defining responsible behaviour in the Defence sector have persisted despite extensive discourse and legislation[31]. The Defence sector evolves with the development of modern warfare, producing more complex technologies and reflecting expenditure on land, maritime, air and cyber capabilities. The Defence sector has also increased in interoperability, reflecting the need to collaborate with other nations in theatre. The Defence sector today is heavily regulated and focused on compliance – concerning the production and exporting of military capabilities. This is not without reason. In relation to defence exports, violating regulations can lead to massive fines, reputational damage[32] and even imprisonment for those found responsible[33].



The core challenge of defining cyber responsibilities reflect similar trade-offs to those in the Defence sector historically: competing interests of the faster-paced private sector in meeting increasing market demands versus establishing robust governance of responsible practices over a longer stretch of time.

The next section looks at what we can learn from the Defence sector's experience in navigating those trade-offs and which ones are translatable for the responsible development of cyber capabilities and capacities.

3 Analysis

3.1 How the Defence industry embeds responsible behaviour

To understand how the Defence industry demonstrates key lessons that could apply to the Cyber sector, we must examine how this industry has embedded responsible behaviour. The Defence industry helps governments protect sovereignty and respond militarily to threats to national and international security. The volume of arms trade has increased throughout the 20th century[34]. Public perception of the Defence industry is nuanced, influenced by global events and ethical dilemmas; sometimes garnering patriotic support during wartime[35] or conversely public outcry, particularly over increasing advancements of capabilities and their potential misuse[36]. Legal controls have grown in line with the landscape of war, in order to ensure appropriate constraints on how industry and governments are able to operate[37]. Corporate responsibility has been supported by the close nature of Defence work between sovereign primes and their national governments – Defence contractors work within the authority of government-issued requirements. As a result, a breadth of precedents and regular practices underpin how the Defence industry can promote responsible behaviour.

Irresponsible behaviours in the Defence industry can stem from non-compliance with export control regulations, supply chain risks, mishandling of sensitive information, and – in more severe cases – corruption or bribery. Though the US Directorate of Defense Trade Controls (DDTC) does not often issue consent agreements, it nonetheless provides a significant route to highlight violations of the US International Traffic in Arms Regulations (ITAR) and penalise defence companies. Consent agreements can be issued for unauthorised exports of goods and information, unauthorised selling and production without licences, or violation of classification and jurisdiction[38]. They provide a means to hold companies to account for improper handling of contracts and are helpful in letting industry know what irresponsible behaviour looks like.

Through the combination of the nature of the Defence industry, the harm to life that military capabilities can pose, and the processes to penalise irresponsible behaviour, industry and government have prescribed strong business practices that are ingrained into regular activities of both the customer and Defence supplier. In the UK, the Defence and Security Public Contracts Regulations 2011 (DSPCR) outlines the special rules and environment in which contractors must align with national security interests and meet requirements for procurement[39]. These regulations set a baseline for contractors in establishing robust business practices. If contractors fail to develop appropriate infrastructure to handle sensitive information, ensure compliance with legislation and licencing requirements, they may not be considered for future contracts.

One interviewee judged that there were wider benefits to responsible behaviour that influence business behaviour. Ensuring compliance with legal requirements and contractual obligations is not just about maintaining a licence to operate, but is vital to maintaining shareholder and public trust while safeguarding international and national security[40]. This is likely to be applicable to cyber companies as well.

The following sections consider how legal and non-legal tools, as well as international cooperation, can influence and promote responsible behaviour in Defence, and – where possible – draw out potential implications for the Cyber sector.

3.2 Legal approaches to influencing responsible behaviour

This section focuses on how the Defence industry has been regulated and considers how the Cyber sector can be influenced by the same legal tools. Both Defence and Cyber regulations are underpinned by a breadth of legislation within the UK, as well as international norms and standards. This provides the foundations for defining what responsible behaviour looks like for government and industry. Much of the legislation extends responsibility to companies on misuse and non-compliance, adapting over time to broaden what is acceptable.

To understand how definitions of responsibility are promoted within the Defence and Cyber sectors, it is worth considering the range of major legislation and agreements, both in the UK and internationally:

Framework	Defence	Cyber
Enabling continued safeguarding of capabilities	• Arms Control Treaties • UN Security Resolutions- notably pertaining to controls on new capabilities, including CBRN[41] [42] • UK Export Control Act 2002[43] & Export Control Order 2008[44]	• Product Security and Telecommunications Infrastructure Regime 2024 (UK)[45] • NIS Regulations 2018 (EU)[46] • EU Cybersecurity Act[47] • Export Control Order 2008[48]
Deterring misuse and irresponsible behaviour	• Geneva Conventions[49], notably the banning of capabilities used to harm non-combatants • US International Traffic in Arms Regulations 1976[50]	• Computer Misuse Act 1990[51] (UK) • Investigatory Powers Act 2016 (UK)
Laws that protect human rights and citizen data	• International Legal Protections of Human Rights in Armed Conflict[52]	• Data Protection Act 2018[53] (UK) • General Data Protection Regulation 2018[54] (EU, UK) • Human Rights Act 1998 (UK)

Understanding legislation across Defence and Cyber is important when determining the motivations for placing protections on developing and using capabilities. Legislation pertaining to Defence – namely the use and misuse and development and sale of defence capabilities – has evolved with the changing landscape of war (including the use of nuclear and chemical). Internationally, UN Security Resolutions have kept pace with the geopolitical landscape of capability development, while state-based policies have ensured that businesses develop and sell responsibly[55]. As a result, there is a breadth of domestic and international legislation which underpinned the nature of military capabilities, seeking to reduce harm to civilians and oppression.

UK Cyber legislation is also multi-faceted. It is underpinned by the right to data privacy[56] and, via regulations such as the NIS Regulations (Security of Network & Information Systems), the protection of essential services through the safeguarding of data confidentiality, integrity and availability. This drives both the requirement for robust cyber security on electronic devices and systems and the misuse of cyber tools to violate privacy, including ransomware and intrusion capabilities. Businesses are held to account for how they handle data and manage interactions across cyberspace.

Cyber security regulation serves to mitigate risks on businesses and individuals in handling data, while misuse – such as unauthorised hacking[57] – is prohibited under national law. The Computer Misuse Act 1990 serves as the foundation for preventing cyber intrusion in the UK[58]. Firms operating in both sectors noted, however, that it is difficult to ensure Responsible Cyber Behaviour – in its broadest sense – through legislative means alone[59].

Comparing Defence and Cyber legislation highlights how both sectors have evolved in reaction to misuse and the risks posed by capabilities as they develop. As a result, nuances across the breadth of legislation in these sectors reflect how the definitions of irresponsible behaviour have adapted over time.

They also reflect how companies in both the Defence and Cyber sectors must navigate and understand the evolution of legislation in order to stay compliant when developing and selling their respective capabilities.

Enforcement and penalties for non-compliance with Cyber regulation can also be costly and risk reputational damage to providers and services. Like Defence-related legislation, Cyber regulation is designed to protect the availability and integrity of technologies – particularly in critical sectors. In the UK, General Data Protection Regulation (GDPR) controls not just the use of personal data, but also the transfer of information and mishandling[60]. Coupled with the Privacy and Electronic Communications Regulations (PECR), cyber service providers must ensure compliant security infrastructure[61]. Fines for mishandling data, violations of network security laws and breaches of GDPR are not uncommon across all industries, with Meta topping the list with a $1.3 billion fine for illicit transfers of personal data from the EU to the US in 2023[62]. Amazon also faced a $877 million fine for breaches of GDPR for using personal data to run targeted advertisements to users[63]. While these were corporate violations of cyber regulation, these penalties serve as precedent for cyber services operating in the public sector.

Other legal mechanisms also help us understand how states view Responsible Cyber Behaviour. One example from 2021 involved information gathering software called Pegasus, in which malware produced by the NSO Group was used to hack into smartphones resulting in the leak of personal data from 50,000 phone numbers[64]. After a lengthy investigation, the NSO Group was found liable and subject to sanctions, including being placed on the US Commerce Entity List for acting “contrary to the foreign policy and national security interests of the US”, thereby restricting its access to US technology[65]. The Pegasus case highlights how governments can enforce more severe penalties beyond fines, ensuring effective sanctions in absence of clear breaches of Cyber regulation. The Pegasus case, alongside the numerous penalties faced by larger service providers, highlights the necessity for clearer controls on the handling of cyber capabilities in line with those in the Defence industry.

While the impact can be severe, the enforcement of regulations serves to change behaviours and highlight the need to be transparent about both responsible and irresponsible behaviours as a precedent for the industry.

3.3 The role of export control in driving responsible behaviour

One approach to understanding responsibility in the use, misuse, development and sale of cyber and defence capabilities is through an examination of export control regulation. Necessary to ensuring responsible selling, end use and destination of exported products and services, export control enables strict enforcement of compliance and clear penalties for misuse. The UK – like the US and EU – upholds an extensive set of export control regimes to ensure that the sale of capabilities (including dual-use items, weapons of mass destruction and other military equipment) does not violate international law or undermine UK national security[66]. In 2017, global arms exports rose to $32 billion, the highest since the collapse of the Soviet Union[67]. Critical to this is the issuing and monitoring of licences. Exporters must apply for licences to develop and export new capabilities and ensure they are:

- Preventing unauthorised exports of defence articles, including technical data
- Preventing unauthorised exports of sensitive information to foreign employees
- Ensuring goods and services are supplied to their intended destination, for the intended end use
- Complying with international obligations, including foreign policy and diplomatic agreements.

Breaking export control licensing rules can result in serious penalties, including sanctions, consent agreements and fines. Interviewees for this paper noted that robust enforcement drives accountability and strong controls to prevent violation. They also noted that the loss of public reputation, financial repercussions and distrust with government stakeholders incentivise reforms by Defence companies to minimise the risk of future export control breaches.

The US ITAR has been used to serve penalties for irresponsible trading in the Defence sector, which can include billion-dollar charges to resolve bribery and control violations. Such penalties centre accountability on sovereign states and create controls for industry in developing capabilities in line with international human rights laws.

The development and distribution of cyber capabilities are also subject to a set of complex export control regulations. Cyber products can be utilised by a wider base of state and non-state end users, so ensuring that their export is legally underpinned is paramount for suppliers. The Export Control Joint Unit operates a ‘catch and release’ process to support the issue of export licences for cyber products, where cyber products are subject to catch-all controls[68] if they could involve breaches of international law[69]. Exemptions are then issued to elements of capabilities that do not pose risk as the technology is consolidated, for instance, whether the physical goods the product is embedded in is subject to controls is dependent on its encryption and other factors[70]. Furthermore, the robust regulation around CMA and its complementary regulation serves as a strong mandate for organisations to remain responsible in producing cyber products, and common practices for handling data on their infrastructure.[71]

3.4 The limitations of export control as a means of regulation

The relationship between Defence companies and their customers is also dependent on export control regulations, especially for end use jurisdiction. Differing export control regimes present different jurisdictional requirements for firms to meet. Though clear on what can and cannot be exported and where, UK export licence controls do not include end use monitoring or approval for third-party selling once it has been exported[72]. This presents additional considerations for Defence companies in developing and exporting a product, particularly concerning potential misuse. One interviewee noted that to manage the challenge of assessing risk posed by misuse and the likelihood of onward transfer, some Defence companies have established clear guidance to staff and an exceptions process that involves additional scrutiny in more complex cases (e.g. those involving a new capability or market) to help identify factors of international humanitarian law that might be affected by a new licence[73].

By comparison, exporting cyber capabilities – including issuing of licenses – can also be complex when determining end use jurisdiction. One interviewee noted that determining the impact of a cyber capability can be uncertain, especially in transfers of technologies[74]. To combat some of this ambiguity, one firm interviewed for this paper uses a distributor system to ensure localised awareness of end destination and end use, providing them with additional expertise to maintain compliance[75]. This external support can help firms to manage multiple compliance regimes.

In a similar vein, ambiguity surrounding jurisdictions is present within cyber export control. Navigating differing encryption and data handling requirements is key to maintaining responsible production of cyber capabilities. The approach of 'catch and release' in cyber export control is inherently different to the Defence model, where there are clearer definitions of what is controlled from the outset[76]. This approach is understandable given the speed at which cyber capabilities are developing. But nonetheless, it creates challenges in understanding what does and does not require an export licence. The private sector is regularly called upon to assist in placing export controls on cyber capabilities, utilising technical expertise to support judgements on licences[77].

The future of cyber export control is still largely undetermined, with questions of ambiguity around dual-use and open source technology[78]. The problem of accountability across multiple jurisdictions is also present in Cyber. For example, relicensing software products creates some ambiguity over data protections and compliance checking[79]. Consideration by the Pall Mall process of multi-stakeholder and multi-jurisdictional challenges associated with enforcing control over offensive cyber product sales should help bring much needed definition here.

In order to reach the maturity of defence export control, the Cyber sector must have a defined scope of controlled services and capabilities, particularly in defining prerequisite security and controls for technology transfers that incorporate sensitive data[80]. Ambiguity within cyber export control – namely for intrusive cyber tools – may lead to violations, whether intentional or unwittingly.

To combat this ambiguity, **effective stakeholder collaboration involving industry, government and academia** can help to share learnings from the Defence industry to support responsible behaviour in cyber export control.

3.5 Non-legal approaches to influencing responsible behaviour

Ethics, transparency measures, and collaboration play central roles in responsible behaviour in the Defence industry. These approaches have been shaped by historical events, non-legal doctrines, politics and public sentiment. As societal standards continue to evolve, ethical considerations increasingly influence how the public view the actions and ethos of both private and public Defence organisations. Change can be driven through unwritten cultural perceptions or through socially accepted standards such as war theories, military doctrines and international agreements, as well as the risk to organisational reputation. While the legal system reflects ethical viewpoints which delineate Defence industry conduct, it does not remove grey areas that divide public opinion, regardless of legality. In addition, organisational standards, policies and guidelines within the Defence sector can be utilised to address gaps in the law. **As a result, organisations use non-legal tools beyond legal requirements to uphold transparency and accountability of Defence contractors, to maintain responsible behaviour.**

The following table captures some non-legal tools discussed within this paper:

Framework	Defence	Cyber
Doctrines and Ethics	• Just War Theory[81] • UK Defence Doctrine[82]	• Allied Joint Doctrine for Cyberspace Operations [83] • Responsible Cyber Power in Practise
	• Non-profit organisations & trade bodies (e.g. TechUK)	
Transparency and communication within industry		• Government advice, e.g. via NCSC UK
	• Public-private consultation e.g. via the Department for Business and Trade and the Export Control Joint Unit (ECJU)	
		• Paris Call • Pall Mall Process[84] – collaboration across industry and internationally led agreements and standards outside the legal framework
Export control agreements	• Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies[85] • Export Control committees/governing bodies	
Governance	• Organisational policies and processes	
		• Cyber related training e.g. Data Protection Act training and cyber security awareness[86]

The role of ethics

Theories and doctrines have evolved over the course of history to define moral conduct in traditional warfare[87]. Though cyber operations are relatively new compared to kinetic tools, their impact is being considered with reference to a similar set of ethical principles. In Defence, Just War Theory addresses 'the justification of how and why wars are fought,' in which the rules of just conduct are assessed through the 'two broad principles of discrimination and proportionality.'[88]

Similarly, the British Army has developed military doctrines which codify 'best practice, based on enduring principles (…) from history and validated lessons from experience and operations' highlighting the importance of applying ethical values through lessons learned[89]. In relation to cyber operations, the UK's National Cyber Force determines that the 'strict adherence to robust legal and ethical frameworks' is also vital[90]. NATO's Doctrine for Cyberspace Operations requires Law of Armed Conflict principles of 'military necessity, humanity, proportionality' to be applied, with 'interference with critical infrastructure or functionality, severity and reversibility of effects' considered. This parallels traditional warfare ethical standards of proportionality and legitimacy.[91]

Collaboration across industry

Research conducted through interviews for this paper suggests that large Defence organisations typically do not distinguish between defence and cyber tools when considering aspects of responsible behaviour[92]. Some industry interviewees questioned whether firms without a long history of export control compliance followed the same approach. Potential reasons that were posited for differences in approach might include company size and experience – with larger Defence firms arguably able to access more resources to invest in regulatory expertise, compliance functions, and company-wide training and oversight than smaller Cyber start-ups. Others questioned whether international regulators had the capacity to drive consistent standards and noted that some firms could use the disparity in common practices to their commercial advantage, such as by operating from national jurisdictions judged to have more permissive export control regimes[93]. One approach to support smaller firms is the use of trade bodies and sharing of best practices. TechUK[94] has created a network of Cyber and Defence firms to connect and discuss practical solutions to barriers in the industry, going as far as establishing committees to build common frameworks of corporate responsibility[95].

This valuable initiative highlights how the private sector can work collaboratively to establish common practices that engrain responsibility across the industry – with more experienced organisations willingly sharing their learnings to benefit the sector as a whole.

The importance of transparency and public opinion

Brand reputation is crucial in an age when '86% of consumers believe authenticity is vital in deciding which brands they like and support[96].' While government-to-government agreements underpin the international Defence industry, and investors typically care about where companies are based and who they sell to[97], reputations built on responsible practices can set an organisation apart. Linked to this, Defence companies are aware that a product ending up in the hands of an unintended or controversial third-party can lead to irresponsible use, damage company reputation and impacting share prices in an already specialised market[98]. While defence capabilities are not sold to the public, public and investor perceptions of the Defence industry impacts share price[99]. As well as influencing government policy and investor sentiment, a reputation for ethical conduct also has a significant impact on recruitment and retention – vital to long-term commercial success.

Events shape public perception, both for the Defence and Cyber sectors. For Defence companies, conflict may heighten awareness of what capabilities are developed and their end use[100]. Whether this perception is positive or not, the Defence sector remains vital due to the necessity of a strong defence versus potential human rights violations. For the Cyber sector, much of public perception is intertwined with the impact of cyber and digital capabilities in global civil society. Following the Pegasus case, the NSO Group's share price was deemed 'valueless' by investors[101], highlighting the public reaction over irresponsible use of cyber capabilities. This presents an interesting comparison, wherein the growing Cyber sector may seem more volatile to shifts in public opinion, however it reflects the societal value shifts present in defence too[102]. As the Cyber sector and public understanding of its capabilities continues to grow, similar discourse surrounding the critical role of Defence in national security interests may be reflected into Cyber.

Embedding standards in business operations

While legal requirements define business activities and conduct in the Defence sector, such as the export of military platforms and capabilities, organisational standards, policies and guidelines address gaps in the law and reduce potential ambiguity and confusion for individuals who work under the remit of laws regarding the Defence sector. Interviewees noted that creating and maintaining clear and accessible standards, policies and processes that reflect societal ethics and organisational values provides clear expectations for staff[103]. Supported by training, individuals can utilise these tools to embed responsible behaviour and accountability in daily operations.

As well as complementing legal requirements, organisational processes and policies also help address staff expectations of their employer; with a more ethically aware workforce many employees do take into consideration the impact their work has on the local community and wider public. Company processes and guidance are also relatively simple to update and so can also help firms adjust dynamically to changes – e.g. to accommodate technological advancements within company policies – more quickly than regulation.

A structural approach to responsible behaviour

Defence organisations also use resources like collaboration groups, ethics committees and end-destination assessments to guide their approaches to capability development and exports[104]. Through assessing the risks associated with end use and destination, ethics committees can evaluate potential misuse and reputational concerns before conducting sales. Lawful products may be rejected if they breach ethical principles, regardless of whether the sale is lawful and requested by the customer. Defence organisations interviewed as part of this paper utilise export control committees or governing bodies to review how trading principles are applied, to both comply with legal requirements and to abide by ethical principles set out by the organisation.

Companies may utilise second-party distributors to ensure export control requirements have been met. This is especially critical considering the challenge Defence organisations face with differing ethical perspectives and freedoms across the international landscape. National and international collaboration fosters responsible behaviour; transparency between industry partners through knowledge sharing and open communication with the aim of developing the Defence industry in turn encourages the adoption of new practices and ethical changes[105]. Training and awareness events with small to medium enterprises, whose users are twice more likely to encounter threats than at large organisations[106], promote knowledge exchange between organisations of various sizes – each serving different perspectives by managing different customer types.

Finally, Defence organisations collaborate closely with government, notably the Export Control Joint Unit (ECJU) and wider government bodies such as the Department for Business and Trade (DBT).

Incorporating experts from industry, policymakers and academia to create a forum to share best practice may encourage more meaningful dialogue and collaboration to understand what it means to be responsible.

4 What lessons can we learn from Defence?

The development of principles and processes in the Defence sector to govern the sale of military capabilities has been largely influenced by legal and non-legal mechanisms, setting the precedent for Defence contractors to establish concepts of responsible behaviours. While this process is not perfect, the large and evolving discourse and the high barrier to entry to secure business in this sector have influenced the concept of responsibility over time. These influences can be adopted into a wide framework of responsible cyber, particularly in offensive cyber, and to tackle proliferation of cyber intrusion capabilities that violate national and international privacy laws.

Significant work has been invested in defining cyber norms at an international level, and – in the UK – making clear that Responsible Cyber Behaviour means avoiding indiscriminate harm in cyberspace, building public trust through effective cyber security practices, transparency, and safeguarding data, and working collaboratively to build a global consensus[107]. **Despite this, it seems likely that further effort is required to help firms understand how to create business governance and structures that embed responsible behaviour to support the responsible production and sale of capabilities.**

Through our review of the Defence sector, this paper suggests that the following lessons relating to the mechanisms that define responsible behaviour are worth considering in the cyber context:

1

Regulation

International agreements have shaped common principles of responsible behaviours, but ultimately domestic legislation is vital to enforce accountability. The industry experts engaged as part of this research are aware of the potential impact of cyber goods and services, their potential for misuse, and the value of controls, but cautioned that the nature of cyber means the fast-paced changes raise questions as to whether export control regulation covering cyber is agile enough to keep pace. Ambiguity could easily create scope for intentional or unwitting violations, and so guidance must continue to be updated to ensure regulation remains aligned. Incorporating Responsible Cyber Behaviour into education and training could help to build understanding of potential violations, and how to capture the correct controls into technologies. A sharing of common irresponsible actions could support the growth of industry code of practise.

2

Enforcement

Through the continuing enforcement of regulations – including fines, sanctions and consent agreements – commercial understanding of responsible behaviour will continue to grow. As well as publicising violations, which have both a deterrent and educational effect, enforcement bodies could collect and publish statistics on the nature and frequency of violations[108]. This could help firms prevent common avoidable mistakes and grow understanding of the nature and extent of cyber capabilities covered by export regulations.

3

Transparency

As a consequence of enforcement action, public and parliamentary scrutiny, and an awareness of the value of public, academic and third sector engagement, numerous Defence firms publish details of their business practices. As well as building confidence, this helps firms understand and reinforce commercial norms. From examining the frequency of consent agreements issued for Defence firms in failing to control the movement of goods and sensitive information, we conclude that ensuring transparency through operational and business practice is key[109]. Building transparency so that users and industry understand regulations and misconduct is an important lesson for Cyber, including through responsible cyber capacity building and cyber security infrastructure.

4

Governance

Effective governance structures are key to conducting responsible business. Stakeholder interviews noted that larger firms have more capacity to build these governance structures that embed due diligence. Smaller organisations potentially have less capacity to build a suitable corporate ecosystem through training, compliance and auditing. The integrated nature of the Cyber sector and larger firms' inevitable reliance on smaller Cyber firms, creates a mutual incentive to increase the cross-pollination of best practice across established players and younger organisations. This can be supported by industry bodies able to facilitate sharing and the development of strong governance mechanisms.

5

Collaboration

Standardisation of responsible behaviour beyond legal compliance has yet to be established within the Cyber sector. Positive steps have been made – including through recommendations in the Pall Mall Process[110]. Setting standards for conduct within industry through utilisation of a wide arena of actors is essential for building an open, peaceful and stable cyberspace. Recognising that Responsible Cyber Behaviours contribute to the health of civil society, it is necessary that regular collaboration across the multi-stakeholder landscape – involving industry, government and academia – continues to keep up with the evolution of Cyber. Academia can help evaluate emerging risks and provide ongoing analysis, while industry has real-world experience of the current threat landscape and government owns the operational requirements. The creation of a forum for the sharing of challenges and exchange of good practice within and across both the Defence and Cyber industry could further contribute to the development of appropriate corporate norms for each sector. Amidst increased geopolitical tensions and competing interests, significant impact could be achieved through the adoption of a common framework developed by and agreed upon by the above parties to define responsible corporate behaviour in this arena.

Click here to learn more about the Global Partnership for Responsible Cyber Behaviour (GP-RCB)

GLOBAL PARTNERSHIP FOR RESPONSIBLE CYBER BEHAVIOUR

Click here to learn more about today's strategic challenges in cyberspace

A Annex A

A.1 Responsible behaviour in practice

Engagement with industry experts as part our research showed that while some firms have defined responsible behaviour in their business policies, others have not. The summary below attempts to capture common factors that can help drive responsible behaviour raised in interviews and identified during research for this paper.

Clearly defined governance	Governance models should define accountability, authority and responsibility for tactical, operational and strategic decisions to ensure effective risk awareness and management.
Embedding responsible behaviour in company policies	Codes of conduct and other policy documents detailing responsibilities, supported by clear processes and procedures, help staff know what should be done. They should be accessible and be promoted and role-modelled by senior leaders to all staff and updated regularly.
Mandatory training and awareness	Corporate training should define acceptable behaviour for all staff, be scenario-based to resonate with real world changes, mandated to all employees, and be conducted, exercised, and practiced regularly to build a responsible culture.
Clear criteria and guidance to enable compliance	Practical guidance and governance structures should enable capability development and sales teams to understand and assess: • Legal and regulatory commitments • Levels of intrusion and collateral damage associated with a product or service • The potential for unintended consequences of a product or service • Customer and end user operating environments (e.g. level of political or judicial freedom)
Pro-active due diligence	Embedded in processes, due diligence should encompass the evaluation of: • Buyers at an individual and business level • End user operating environments (e.g. government and political levels) • Supply chains
Provision of internal reporting mechanisms	Enable staff to whistle blow on irresponsible behaviour by providing accessible, confidential channels for raising ethical and business conduct concerns. This should be supported by mechanisms to investigate and act upon the information received – be it related to the business, supplier or customer.
Processes for reporting irresponsible behaviour to regulators	Simple self-referral mechanisms ensure firms that identify potential irresponsible behaviour or mistakes can engage regulators promptly for guidance and action as appropriate.
Pro-active and dynamic collaboration	Open dialogue and regular knowledge sharing across industry with trade bodies, government, and international partners strengthens understanding, builds common standards, and allows more experienced firms to help younger and smaller firms ensure they behave responsibly.

References

[1] Department for Science, Innovation, & Technology Research and Analysis (2025) Cyber security sectoral analysis 2025

[2] Understanding Cyber Effects in Modern Warfare - War on the Rocks

[3] United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (2015) proposed norms of responsible cyber behaviour

[4] This definition is drawn from the UK Department for Science, Innovation and Technology analysis of the cyber security sector. See UK Cyber Security Sectoral Analysis Report 2025

[5] Open-ended working group on information and communication technologies (2021) | United Nations 2020-2025

[6] 'The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities' February 2024, Foreign, Commonwealth and Development Office

[7] Cybercrime Trends 2025 | Report

[8] Prime Minister sets out biggest sustained increase in defence spending since the Cold War, protecting British people in new era for national security - GOV.UK

[9] The UK is a Global Cyber Power, says Director GCHQ - GCHQ.GOV.UK

[10] Devanny J., Dwyer A., Ertan A., Stevens T. (2021) 'The National Cyber Force that Britain Needs?' Cyber Security Research Group, Offensive Cyber Working Group, Kings College London

[11] Responsible_Cyber_Power_in_Practice.pdf

[12] How the EU is strengthening its cybersecurity - Consilium

[13] How the EU is strengthening its cybersecurity - Consilium

[14] Department for Business and Trade and UK Defence and Security Exports (2024), UK defence exports statistics 2023

[15] Top defence companies by revenue Europe | Statista

[16] Defence and Security Exports and Department for Business and Trade (2025), UK security exports statistics 2023

[17] UK arms exports: statistics - House of Commons Library

[18] See Department for Science, Innovation, & Technology Research and Analysis (2025) Cyber security sectoral analysis 2025; and Cyber security Export Strategy, (2018) Department for International Trade

[19] UK security export statistics 2023 - GOV.UK (2023), UK Defence and Security Exports, UK Department for Business and Trade

[20] Guidance - Defence and Security Contracts (HTML) - GOV.UK

[21] Defence and Security Exports and Department for Business and Trade (2025), UK security exports statistics 2023

[22] Global Compendium on Responsible Cyber Behaviour | Royal United Services Institute

[23] E.g., OECD (2002), Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

[24] NATO Strategic Communications Centre of Excellence: 2007 cyber attacks on Estonia

[25] E.g., see Understanding Cyberwarfare: Lessons from the Russia-Georgia War - Modern War Institute

[26] E.g., Researchers say Stuxnet was deployed against Iran in 2007 | Reuters

[27] UN General Assembly (2015) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

[28] EU General Data Protection Regulation (2016) General data protection regulation (GDPR) | EUR-Lex

[29] See The call and the 9 principles — Paris Call

[30] See The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities - GOV.UK

[31] Responsible Defence Governance - Transparency International Defence & Security

[32] Stakeholder Interview February 2025

[33] UK Government Export Control Licence

[34] Çağlar Kurç, Stephanie G. Neuman, (2017), Defence industries in the 21st Century: a comparative analysis' Defence Studies Vol. 17, No.3 219-227

[35] Military Dispatches Editorial (2024) 'Public Perception and Its Impact on the Defense Industry' Military Dispatches DOI: Public Perception and Its Impact on the Defense Industry - Military Dispatches

[36] Spears, R. (2021). The Impact of Public Opinion on Large Global Companies' Market Valuations: A Markov Switching Model Approach. Journal of Finance and Economics, Volume 9. Retrieved from SciEP

[37] See House of Commons Research Briefing (2024) An introduction to UK arms exports for an evolution of Strategic Export Licencing Criteria and House of Commons Briefing Paper (2017) The legal and regulatory framework for UK arms exports for a summary of how events such as the sale of arms-to-Iraq and use of UK-manufactured arms in Yemen by Saudi Arabia have influence the development of export regulation. More widely, the UK Government has introduced a range of legislation to respond to threats to UK national security, e.g., granting government powers in relation to surveillance, detention, and preparedness to tackle terrorism over the last 25 years (such as the Investigatory Powers Act 2016, Civil Contingencies Act 2004, and the Terrorism Act 2000) and – much earlier – in 1914 both the Emergency Powers Act and the Defence of the Realm Act

[38] US Department of State, Directorate of Defence Trade Controls, Penalties and Oversights Agreements DDTC Public Portal

[39] Guidance - Defence and Security Contracts (HTML) - GOV.UK

[40] Stakeholder Interview February 2025

[41] UN General Assembly (2023) 'General and complete disarmament: treat banning the production of fissile material for nuclear weapons or other nuclear explosive devices'

[42] UN General Assembly (2022) 'Resolution 2663: concerning the Non-Proliferation of Nuclear, Chemical and Biological Weapons' Adopted by the Security Council at its 9205th meeting on 30 November 2022

[43] 'Export Control Act' (2002) makes provisions for exported goods, transfers of technologies and technical assistance overseas. Export Control Act 2002

[44] The Export Control Order (2008) regulates the exports. Brokering, transfer and transit of controlled goods, software and technology The Export Control Order 2008

[45] The UK Product Security and Telecommunications Infrastructure (Product Security) regime - GOV.UK Businesses in the supply chain of these products now need to be compliant with the legislation, Department for Science Innovation and Technology

[46] The NIS Regulations 2018 - GOV.UK Providing legal measures to boost the level of security (both cyber and resilience) of network and information systems for the provision of essential services and digital services, Department for Digital Culture, Media and Sport

[47] The EU Cybersecurity Act | Shaping Europe's digital future introduces an EU-wide cybersecurity certification framework for ICT products, services and processes. Companies doing business in the EU will benefit from having to certify their ICT products, processes and services only once and see their certificates recognised across the European Union

[43] 'Export Control Act' (2002) makes provisions for exported goods, transfers of technologies and technical assistance overseas. Export Control Act 2002

[44] The Export Control Order (2008) regulates the exports. Brokering, transfer and transit of controlled goods, software and technology The Export Control Order 2008

[48] The Export Control Order (2008) regulates the exports. Brokering, transfer and transit of controlled goods, software and technology The Export Control Order 2008

[49] 1997 Anti-Personnel Mine Ban Convention, the 2003 Protocol on Explosive Remnants of War (an addition to the 1980 United Nations Convention on Certain Conventional Weapons) and the 2008 Convention on Cluster Munitions

[50] 'International Traffic in Arms Regulation' (1976) ensures commercial exports of defence advance US national security and foreign policy objectives, and is governed by the Arms Control Export Act. Article - DDTC Public Portal

[51] Computer Misuse Act 1990 UK law that criminalizes unauthorized access to computer systems and data

[52] International Legal Protection of Human Rights in Armed Conflict | OHCHR

[53] Data Protection Act 2018 Responsibilities for using personal data under the 'data protection principles'

[54] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation) (Text with EEA relevance)

[55] Ibid

[56] Clark A. (April 2024) 'Cyber Security in the UK' House of Commons Library

[57] Authorised hacking – such as the activity of an EC-Council Certified Ethical Hacker) encompasses lawfully looking for vulnerabilities in systems using the tools and techniques employed by malicious hackers

[58] BAE DI Industry Research (February 2025)

[59] BAE DI industry research (February 2025)

[60] UK GDPR Guidance and Resources, Information Commissioner's Office Consent | ICO

[61] 'What are PECR, Information Commissioner's Office What are PECR? | ICO

[62] The biggest data breach fines, penalties, and settlements so far | CSO Online

[63] GDPR infringement: Luxembourg court confirms record fine for Amazon | heise online

[64] Pegasus spyware scandal: what lawyers need to know | infolaw CPD training

[65] Unpacking WhatsApp's Legal Triumph Over NSO Group | Lawfare

[66] The UK's Export Control Act 2002 forms the basis of this export control system

[67] Mandle, L. J., & Pearson, F. S. (2023). International arms trade and transfers: Rising producers, advanced technology, and adapting regulations. International Journal, 78(1-2), 60-86. https://doi.org/10.1177/00207020231179054 (Original work published 2023)

[68] 'Catch all controls' refers to the ECJU model for placing export controls on cyber capabilities, to cover items not necessarily on the dual use list. This method is inherited from EU export control regulation

[69] Stakeholder Interview February 2025

[70] Software Export Controls between the EU and the UK – the Impact of Brexit - Bird & Bird

[71] Stakeholder Interview February 2025

[72] Stakeholder Interview February 2025

[73] Stakeholder Interview February 2025

[74] Stakeholder Interview February 2025

[75] Stakeholder Interview February 2025

[76] ECJU Interview (March 2025) & BAE DI industry research (February 2025)

[77] ECJU Interview (March 2025)

[78] Stakeholder Interview February 2025

[79] Stakeholder Interview February 2025

[80] Stakeholder Interview February 2025

[81] E.g. see Cian O'Driscoll (2015) Rewriting the Just War Tradition: Just War in Classical Greek Political Thought and Practice

[82] Ministry of Defence, 2022, 'UK Defence Doctrine (Sixth Edition)' UK Defence Doctrine (JDP 0-01) - GOV.UK

[83] NATO, 2020, 'Allied Joint Doctrine on Cyberspace Operations'

[84] Foreign Commonwealth Development Office, February 2024, 'The Pall Mall Process'

[85] E.g. see 'Best Practises for Effective Export Control Enforcement' Agreed at the 2000 Plenary. The Wassenaar Arrangement is a voluntary multi-lateral arrangement supporting control lists for dual use and conventional arms

[86] See: Information Commissioner's Office site for training and awareness relating to the Data Protection Act 2018 DOI: Training and awareness | ICO

[87] E.g., see Cian O'Driscoll (2015) Rewriting the Just War Tradition: Just War in Classical Greek Political Thought and Practice

[88] Spears, R. (2021). The Impact of Public Opinion on Large Global Companies' Market Valuations: A Markov Switching Model Approach. Journal of Finance and Economics, Volume 9. Retrieved from SciEP

[89] Ibid

[90] The National Cyber Force: Responsible Cyber Power in Practice

[91] Allied Joint Doctrine of Cyberspace Operations-3.20

[92] Stakeholder Interview February 2025

[93] Stakeholder Interview February 2025

[94] The UK's technology trade association, TechUK are a defence and cyber trade body that empower a range of large and small firms to share best practices across industry, particularly in championing future growth and resilience against change

[95] Stakeholder Interview February 2025

[96] Spears, R. (2021). The Impact of Public Opinion on Large Global Companies' Market Valuations: A Markov Switching Model Approach. Journal of Finance and Economics, Volume 9. Retrieved from SciEP

[97] E.g., see 94% of investors consider defence stocks ESG friendly | Portfolio Adviser

[98] Stakeholder Interview February 2025

[99] Spears, R. (2021) The Impact of Public Opinion on Large Global Companies' Market Valuations: A Markov Switching Model Approach. Journal of Finance and Economics, Volume 9. Retrieved from SciEP; see also the change in investor attitudes to the Defence sector in light of the Ukraine war e.g. 94% of investors consider defence stocks ESG friendly | Portfolio Adviser

[100] Public Perception and Its Impact on the Defense Industry - Military Dispatches

[101] Unpacking WhatsApp's Legal Triumph Over NSO Group | Lawfare

[102] Public Perception and Its Impact on the Defense Industry - Military Dispatches

[103] Stakeholder Interview February 2025

[104] Stakeholder Interview February 2025

[105] Stakeholder Interview February 2025

[106] Mimecast Global Threat Intelligence Report Q4 2023

[107] See for example, the UK National Cyber Strategy 2022 and National Cyber Force (2023) Responsible Cyber Power in Practice

[108] See the US Government Accountability Office report on export controls (2023) for an example of the challenges with statistical data in relation to compliance

[109] US Department of State, Directorate of Defence Trade Controls 'Penalties and Oversights' Article - DDTC Public Portal

[110] 'The Pall Mall Process' February 2024, Foreign Commonwealth and Development Office

We are Digital Intelligence

BAE Systems Digital Intelligence is home to over 4,700 digital, cyber and intelligence experts across 16 countries. We operate at the cutting edge of digital innovation and at the heart of organisations that keep vital infrastructure running, national security protected and armed forces prepared.

Our teams provide advanced digital capability, products and solutions that weave together digital threads of data so that customers get the vital insight they need – from the fine detail to the bigger picture, providing the power of perspective to confidently make the critical decisions that keep our societies safe and able to thrive.

Digital Intelligence is a part of BAE Systems and has a rich heritage in helping to defend nations and businesses around the world from advanced threats. Whether on land, in the air, at sea, in space or cyberspace, we're your digital mission partner, with you every step of the journey.

BAE Systems Digital Intelligence
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems Digital Intelligence
Level 2
14 Childers St
Canberra
ACT 2601
Australia
T: +61 (0) 2 9053 9330

BAE Systems Digital Intelligence
Malta Office Park
ul. Abpa A. Baraniaka 88
Poznan
61-131
Poland
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence
Level 28, Menara Binjai
2 Jalan Binjai
Kuala Lumpur
50450
Malaysia
T: +60 327 309 390

E: learn@baesystems.com
W: baesystems.com/digital

linkedin.com/company/baesystemsdigital
@BAESystemsDigi

Digital Intelligence

BAE SYSTEMS